

Please enter  
A.N. 05/05/06

**IN THE SPECIFICATION:**

Please amend the Specification as follows.

[0004] The IETF draft (draft-forsberg-pana-secure-network-access-auth-00.txt) presents a link layer independent network access authentication method, Secure Network Access Authentication (SeNAA), to support smooth interaction between user equipment (UE) and access networks while roaming. The draft authentication method has two phases, I and II. Phase I must be completed before phase II can be started. The serial message processing is slow.

[0005] Fig. 1 depicts the original (draft) version of the authentication protocol which was not adopted. Mobile terminals utilize different link layer technologies and roam between different layers. A generic link layer independent authentication and authorization method is needed to support smooth interaction between user equipment ~~UE~~ and access networks while roaming. User equipment ~~UE~~ network access authentication in different network technologies has become an important issue in the Internet. Different authentication methods already exist but are more or less link layer dependent.

[0006] Secure Network Access Authentication ~~SeNAA~~ uses User Datagram Protocol (UDP) as the transport protocol. UDP is a lightweight protocol and allows application level implementations with port numbers UDP carries DIAMETER formatted Secure Network Access Authentication ~~SeNAA~~ messages. Secure Network Access Authentication ~~SeNAA~~ provides reliable request and response style message delivery (re-transmission and duplicate packet detection).

[0007] Secure Network Access Authentication ~~SeNAA~~ does not assume a secure channel

between Protocol for carrying Authentication for Network Access Authentication (PANA) Client (PaC) and PANA PANA Authentication Agent (PAA) PaC and PAA. Thus, on top of the Secure Network Access Authentication ~~SeNAA~~ protocol Transport Level Security (TLS) TLS, a protocol is used to negotiate a Local Security Association (LSA) between PANA Client PaC and PANA Authentication Agent PAA. Transport Level Security TLS provides authentication, privacy, integrity, and replay protection. Transport Level Security TLS is used to protect Secure Network Access Authentication ~~SeNAA~~ message AVPs and EAP between PANA Client PaC and PANA Authentication Agent PAA. AVPs that need protection are fed to the Transport Level Security TLS Record layer, and the resulting encrypted and compressed data is stored into a TLS-Payload AVP. EAP protocol is carried inside an EAP-Payload AVP. Secure Network Access Authentication ~~SeNAA~~ messages after successful Transport Level Security TLS handshake are integrity protected with a check sum stored in the Msg-Checksum AVP. The AVP is protected with Transport Level Security TLS Record layer.

[0008] Transport Level Security TLS is also used for re-authentication between PANA Client PaC and PANA Authentication Agent PAA. Transport Level Security TLS supports mutual authentication and can optionally be used instead of EAP for user authentication. In all cases Transport Level Security TLS is used for access network authentication. Secure Network Access Authentication ~~SeNAA~~ messages carry information such as the PANA Client's PaC's Device Identifier (DI), that must be integrity protected. If PANA Authentication Agent PAA supports DIAMETER and/or RADIUS Authentication, Authorization and Accounting (AAA) AAA back-end,

signaling between PANA Client PaG and PANA Authentication Agent PAA can easily be extended to the back-end. Secure Network Access Authentication SeNAA doesn't rely on any modifications to the EAP protocol. It provides secure transport up to the PANA Authentication Agent PAA for EAP. Thus, any existing EAP methods can be used securely with Secure Network Access Authentication SeNAA between PANA Client PaG and PANA Authentication Agent PAA. Security after PANA Authentication Agent PAA is outside the scope of Secure Network Access Authentication SeNAA. PANA Authentication Agent PAA is assumed to get user authentication answer (Success or Failure) from the authenticator.

[0009] Secure Network Access Authentication SeNAA utilizes protocols like EAP, TLS, UDP and IP that are assumed to exist in the PANA Client PaG terminal already even without Secure Network Access Authentication SeNAA. Fig. 2 illustrates an exemplary one. DIAMETER like message formatting and request response style reliability transport is one additional requirement for the PANA Client PaG terminal and is provided with the Secure Network Access Authentication SeNAA protocol. TCP and SCTP are considered too heavy weight transport protocols for Secure Network Access Authentication SeNAA purposes (i.e. more message round trips needed).

[0010] Data protection, such as IP datagrams, is out of the scope of Secure Network Access Authentication SeNAA. One possibility for further studies is to use the key material produced in the Transport Level Security TLS handshake process with IPsec.

[0011] With reference to Fig. 1, successful mutual authentication is divided into two phases. In Phase I the network is authenticated, and the user is authenticated in Phase II.

[0012] Phase I consists of a Transport Level Security TLS handshake as is shown in Fig 3A which provides initial authentication with Transport Level Security TLS to provide a secure tunnel. Local reauthentication, where PANA Client PaC authenticates to PANA Authentication Agent PAA, is in Phase I and is handled with Transport Level Security TLS Session Resumption (illustrated in Fig. 3B which provides re-authentication with TLS). Access network authentication is based on access network certificates. How certificates are created, processed and verified is known and not described herein.

[0013] Phase II uses EAP for authenticating the user (Fig. 4 illustrates user authentication signalling with EAP being carried inside the EAP-Payload AVP). User authentication is bound to the DI, which is used to control access to the network. [0014] With reference to Fig. 1, in Phase I, Server-Certificate-Request (SCR) message carries Client-Hello TLS message. Server-Certificate-Answer (SCA) carries the TLS answer which contains the Access Network certificate. PANA Client PaC verifies the certificate. PANA Authentication Agent PAA also adds a Session-Id AVP into the SCA message. This Session-Id is different from the Transport Level Security TLS session-Id. The next messages must have the AVP included during the whole session. To finish the TLS handshake, PANA Client PaC sends Client-Security-Association-Request (CSAR) message to the PANA Authentication Agent PAA. PANA Authentication Agent PAA answers with Client-Security-Association-Answer (CSM).

[0015] When Transport Level Security TLS is not used, a different User Datagram Protocol (UDP) UDP port number (PAA UDP port <UDP-port3>, PaC UDP port <UDP-port4>) must be used for plaintext CLR/CLA message delivery. PANA Client PaC can

decide not to use Phase I authentication but must use Phase I authentication if <UDP-port3> is not reachable. Similarly if UDP port <UDPporti> is not reachable, PANA Client PaC should try to use UDP port <UDP-port3>.

[0016] In Phase II, after a successful TLS handshake, PANA Client PaC uses AAA-Client Request (CLR) message to start user authentication and DI authorization. CLR carries EAP-Payload AVP to PANA Authentication Agent PAA. PANA Authentication Agent PAA answers with AAA-Client-Answer (CLA) message with a Result-Code AVP. Result-Code informs PANA Client PaC if multiple round trips are needed for completing the EAP authentication method or if the authentication (authorization) succeeded or failed.

[0017] PANA Client PaC adds DI(s) thereof into the CLR message so that PANA Authentication Agent PAA can verify the integrity of the DI and optionally provide it for the enforcement point.

[0018] PANA Authentication Agent PAA can be co-located in the ARs or separated from the ARs. In case of separation, ARs act as relay agents to PANA Authentication Agent PAA for MN. PANA Authentication Agent PAA is in the same subnet as the AR and Mobile Node (MN) MN. When PANA Authentication Agent PAA receives a message from Mobile Node MN through an AR, it must send the reply directly to the Mobile Node MN. When PANA Authentication Agent PAA is separated from ARs, an AR should relay MN's Secure Network Access Authentication SeNAA messages to the PANA Authentication Agent PAA. When Mobile Node MN receives an answer from PANA Authentication Agent PAA, the Mobile Node MN must send further requests to

the PANA Authentication Agent PAA directly.

[0019] Secure Network Access Authentication SeNAA uses request and response style transactions. For each request a response is sent. If a response is not received in time, the request is re-sent. This mechanism is used for packet loss recovery. The received response works as an acknowledgment. Secure Network Access Authentication SeNAA uses DIAMETER message formatting. The DIAMETER message header provides packet duplication (End-to-End Id) detection and request/response mapping (Hop-by-Hop Id).

[0020] To protect integrity of the DIAMETER header and the whole message, MAC is calculated over the DIAMETER message. The MAC is put into an AVP called Msg-Checksum. CLR/CLA messages use this AVP. PANA Client PaC needs to be authenticated before network access is granted through the enforcement point (EP) in the access network.

[0021] Authentication and re-authentication initiator can be PANA Client PaC or PANA Authentication Agent PAA.

[0022] PANA Client PaC starts re-authentication by sending CSAR message with Transport Level Security TLS Client Hello in the TLS-Payload AVP to PANA Authentication Agent PAA to UDP port <UDP-port1> (Fig. 3B). Similarly, PANA Authentication Agent PAA initiates re-authentication by sending CSAA message with Transport Level Security TLS Server Hello message in the TLS-Payload AVP to PANA Client PaC to UDP port <UDP-port2>. The hello message contains the current Transport Level Security TLS session specific id, which is used to detect session resumption from initial authentication. Re-authentication involves multiple CSAR/CSAA round trips.

[0023] After a Transport Level Security TLS handshake or session, resumption is done and the SA is established PANA Client PaC uses the Transport Level Security TLS Record Layer to encrypt Secure Network Access Authentication SeNAA message AVPs.

[0024] Secure Network Access Authentication SeNAA doesn't assume connection-oriented links. Thus, Transport Level Security TLS reauthentication is used for notifying PANA Authentication Agent PAA of PANA Client's PaC's presence. Re-authentication interval is implementation specific <TBD?>.

[0025] Transport Level Security TLS Alert, Handshake and Change cipher specification protocols are carried inside Transport Level Security TLS Record Layer. For example if Transport Level Security TLS Alert protocol reports a fatal error it is delivered with the next TLS-Payload AVP or with separate CSAR/CSM messages. The Secure Network Access Authentication SeNAA application must understand the return codes from Transport Level Security TLS Record Layer API functions. When fatal error is received, the Transport Level Security TLS session is torn down. The Secure Network Access Authentication SeNAA session MUST be re-negotiated.

[0026] Transport Level Security TLS message formats can be found from Transport Level Security TLS. The DIAMETER message header format and AVP format is known. SCA and CSM messages do not contain Result-Code AVPs.

[0027] Format of the SCR message:

<Server-Certificate-Request> ::= < Diameter Header: <TBD>, REQ, PXY>  
    { User-Name }  
    { TLS-payload }

TLS-Payload AVP contains the Transport Level Security TLS handshake messages in the AVP data area as specified in [TLS]. The TLS-Payload AVP contains TLS-Client-hello.

Format of the SCA message:

<Server-Certificate-Answer> ::= < Diameter Header: <TBD>, PXY> <Session-Id>  
    { TLS-payload }

A Session-Id is generated for the PANA Client PaC and delivered in the Session-Id AVP. The TLS-Payload AVP contains Transport Level Security TLS Server-hello, Transport Level Security TLS Server-Certificate, TLS server-Key-Exchange, and Transport Level Security TLS Server-Hello-Done messages. Format of the CSAR message:

<Client-Security-Association-Request> :: <Diameter Header: <TBD>, REQ>  
    <Session-Id>  
    { TLS-payload }

The Session-Id AVP is used in every SeNAA message between PANA Client PaC and PANA Authentication Agent PAA.

The TLS-Payload contains TLS-Client-Key-Exchange, TLS-Change-CipherSpec, and TLS-Client-Finished messages.

[0028] Format of the CSM message:

<Client-Security-Association-Answer> ::= < Diameter Header: <TBD>, PxY>  
    <Session-Id>  
    { TLS-Payload }

The TLS-Payload contains TLS-Change-Cipher-Spec and TLS-ServerFinished messages.

[0029] Format of the initial CLR message:

<AAA-Client-Request> :: <Diameter Header: <TBD>, REQ, PXY> [TLS-Payload:  
    <Session-Id> { User-Name } { Device-Identity } [EAP-Payload]  
    [Authorization-Lifetime]  
    [Msg-Checksum]  
]



The TLS-Payload AVP data area contains encrypted AVPs through Transport Level Security TLS Record layer.

[0030] Format of the CLA message from PANA Authentication Agent PAA to PANA Client PaC:

```
<AAA-Client-Answer> ::= < Diameter Header: <TBD>, PXY> [TLS-Payload:
    <Session-Id> { Result-Code } [EAP-payload]
    [Authorization-Lifetime]
    [Auth-Grace-Period]
    [Multi-Round-Time-Out]
    [Msg-Checksum ]
]
```

The TLS-Payload AVP data area contains encrypted AVPs through Transport Level Security TLS Record layer.

[0031] The TLS-Payload AVP data contains encapsulated AVPs that are encrypted and compressed by Transport Level Security TLS Record layer. Upon receive of TLS-Payload AVP the data area is first fed to the Transport Level Security TLS Record layer to get the plain text AVP list for further processing.

[0032] The Msg-Checksum AVP data contains checksum of the whole DIAMETER message. Msg-Checksum is calculated over the message with MsgChecksum AVP data area bits set to zero. Checksum algorithm is <TBD>.

[0033] The CLA message contains Transport Level Security TLS protected Result-Code AVP. In Secure Network Access Authentication SeNAA one of the following Result-Code values is possible.

DIAMETER\_MULTI\_ROUND\_AUTH 1001

EAP user authentication requires more round trips.

DIAMETER\_SUCCESS 2001

EAP user authentication and network access authorization successful.

DIAMETER\_AUTHENTICATION\_REJECTED 4001  
EAP user authentication failure.

[0034] Secure Network Access Authentication ~~SeNAA~~ provides reliable request and response style transactions. Peer which initiates the transaction is responsible for re-transmission if the corresponding response is not received in <TBD-msec> milliseconds. Maximum number of retries is <TBD-retries>.

[0035] If Multi-Round-Time-Out AVP is included in a Secure Network Access Authentication ~~SeNAA~~ message from PANA Authentication Agent ~~PAA~~ to PANA Client ~~PaC~~, the re-transmission (same Hop-by-Hop Id and End-to-End Id) MUST not exceed this time limit.

[0036] UDP Port number(s) must be defined. SCR/SCA, CSAR/CSM and CLR/CLA message command codes must be assigned. Msg-Checksum and TLS-Payload AVP codes must be assigned.

[0037] Fig. 1 as described above illustrates the use of DIAMETER-EAP authentication. In the first step, the EAP client is requested to initiate the authentication procedure. Normally, the client (EAP peer) authentication is requested by the EAP authenticator or an access point, but one round-trip of EAP messages is saved when the client device, which comprises the EAP client, initiates the authentication request (EAP Request (Identity)). The EAP client responds to the request and provides an identity in the response message.

[0038] In the next step, the client or user equipment ~~UE~~ request the server in the access network (access router) to authenticate itself. The client sends a message (client hello in this embodiment where Transport Level Security ~~TLS~~ is used) to the server, the message

containing a session ID and information on the client's supported cryptographic algorithms. The client can indicate in the message, from which certifying authority it wishes the server to acquire its security certificate. The server responds with a server hello message, indicating the selected encryption/validation algorithm, as well as provides a security certificate to the client. The next messages conclude Phase I, establishing a secure connection between the client and the server in the access network. Both the client and the server send a finished message to confirm that the key exchange and authentication were successful.